PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-252069
(43)Date of publication of application : 17.09.1999

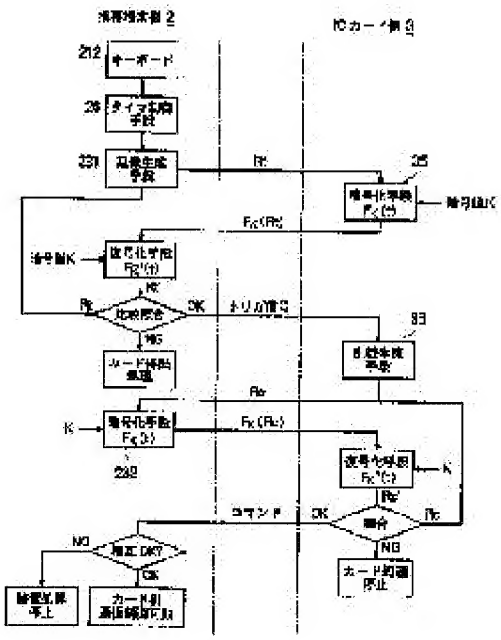
(51)Int.Cl. H04L 9/32
G06F 7/58
G09C 1/00

(21)Application number : 10-054625
(22)Date of filing : 06.03.1998

(71)Applicant : FUJI ELECTRIC CO LTD
(72)Inventor : IKEDA FUMIYUKI

(54) MUTUAL AUTHENTICATION DEVICE BETWEEN INFORMATION DEVICES

(57)Abstract:
PROBLEM TO BE SOLVED: To make an authentication device hardly estimate a measured value due to acquisition of a random value and to improve the reliability of the authentication device by measuring the key depressing time of one of the both devices when they mutually encipher and decode random numbers to authenticate the opposite device and using the measured value as an initial value to generate the random number.
SOLUTION: The random number data which are generated by a portable terminal 2 that has a common enciphering/decoding key are sent to another device such as an IC card 3 or an automatic vending machine 1. The other device which receives the random number data encihpers these data and returns them to the terminal 2. The terminal 2 decodes the received cipher data and compares them with the original random number data. When the coincidence is confirmed between the both data, the device of the opposite party side is decided as a correct device. In such a constitution of this mutual authentication device, the depressing time of a keyboard 212 of the terminal 2 is measured and a random number is generated by using the measured time as an initial value.



LEGAL STATUS

[Date of request for examination] 14.02.2003
[Date of sending the examiner's decision of rejection] 28.02.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] The random-number data which are between two devices which have common encryption/decryption key, and one device generated to the device of another side Delivery, The device of another side which received it enciphers random-number data, and returns them to one device. In the mutual recognition equipment between the information machines and equipment which accept that a phase hand-loom machine is just when a device decrypts code data and while it was received is in agreement as compared with the original random-number data Mutual recognition equipment between the information machines and equipment characterized by having a random-number generation means to measure the depression time amount of the alter operation key which one device has, and to generate a random number by making the value of the measuring time into initial value.
[Claim 2] In the mutual recognition equipment between information machines and equipment according to claim 1, the numeric value of a proper is beforehand held to the device of another side. After random-number data are sent to the device of another side from one device and it is enciphered and returned A device enciphers the numeric value of a proper and while delivery and it were received to one device returns the numeric value of the proper holding the device of another side to the device of another side. The device of another side which received it is mutual recognition equipment between the information machines and equipment characterized by accepting that a phase hand-loom machine is just when code data are decrypted and it is in agreement as compared with the numeric value of the original proper.
[Claim 3] Mutual recognition equipment between the information machines and equipment which use the device of another side as the IC card with which said personal digital assistant can be equipped in the mutual recognition equipment between information machines and equipment according to claim 1 or 2 while using one device as a personal digital assistant, and are characterized by having a bottom time amount measurement means of a key press to measure the bottom time amount of a key press when the alter operation of the ID number to a personal digital assistant is made after IC card wearing, and to input into a random-number generation means.
[Claim 4] The mutual-recognition equipment between the information machines and equipment which use the device of another side as the automatic vending machine in which data transmission and reception are possible by non-contact [said / personal digital assistant and non-contact] in the mutual-recognition equipment between information machines and equipment according to claim 1 or 2 while using one device as a personal digital assistant, and are characterized by to have a bottom time-amount measurement means of a key press measures the bottom time amount of a key press when the alter operation of the ID number to a personal digital assistant is made in the state of both connection, and input into a random-number generation means.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the mutual recognition equipment between the suitable information machines and equipment for the system which collects the sales information on an automatic vending machine, and money information especially using the personal digital assistant with which a route man has infrared communication facility about the mutual recognition equipment between the information machines and equipment used for cybermoney, an electronic clearing system, etc.
[0002]
[Description of the Prior Art] Although the magnetic card has been conventionally used as a pachinko card, a telephone card, etc. as a prepaid card, since security is inadequate, the IC card which has high security is being used so that a magnetic card may also become a social problem by alteration etc. Moreover, the cybermoney using the CPU built-in IC card called a smart card and the system called electronic banking are advocated, and various kinds of experiments are conducted in recent years. There is a system by which a route man collects the sales of the automatic vending machine which can use cybermoney as the example using the personal digital assistant which has infrared communication facility. Specifically, cybermoney here is a pocketbook value memorized to the address of the arbitration of the storage of an automatic vending machine.
[0003] Drawing 1 shows the system concept, is equipped with the automatic vending machine 1 which can be used and infrared communication facility of cybermoney, and consists of an automatic vending machine 1 and IC card 3 held by the individual for whom the personal digital assistant 2 in which the data exchange is possible, and a personal digital assistant 2 are used by non-contact. In this system, the data of the sales and others by the cybermoney of an automatic vending machine 1 are collected by the personal digital assistant 2 by infrared ray communication, and collection of money is made by moving and changing those data to a route man's IC card 3 further. Drawing 7 is the block diagram showing the structure of a personal digital assistant 2 where conventional IC card 3 is inserted.
[0004] A personal digital assistant 2 Overall control CPU21 to perform and its program Even if it memorizes ROM23 and important data to memorize and a power source is shut off The communications control circuit 214 for performing E2ROM24, the transient-data storage memory RAM 25 for program working and IC card 3 which can be saved, and communications control, the clock control circuit 22 which carries out an international standard frequency output control, a reset circuit 215, It is constituted by the power control circuit 216 for carrying out current supply to a card, the interface terminal 221, the indicator 210 that is the user interface section, the display driver 29 for it, and the display-control circuit 28. It has the mutual recognition means 213 for judging that he is an owner with just keyboard 212 for a route man to input the command for automatic-vending-machine data collection, its interface 211, and IC card 3.
[0005] This mutual recognition means 213 will make values, such as that time of day, an initial random-number value with a binary representation, if it points so that a password may be entered from the display screen of an indicator 210 and a keyboard 212 is pushed, when it consists of a random-number generation means 231 and an encryption/decryption means 232 and IC card 3 is inserted by the command from the random-number generation means 231. Moreover, by the result to which encryption/decryption means 232 decrypted the received code, if mutual recognition is materialized, actuation of the communications control circuit 217 will be permitted and the communication by the side of an automatic vending machine 1 will be attained. The communication with an automatic vending machine 1 is equipped with the infrared transceiver driver circuit 218 which are the infrared photogenic organ LED 219, an electric eye PD 220, and its driver circuit in order to

use infrared radiation.
[0006] Whether the system excellent in security by which a route man can collect with justice, without being stolen by the offender, the cybermoney, i.e., the electronic data, transposed to the conventional coin and a bill, is establishable poses a problem here. Therefore, the mutual recognition between IC card 3 and a personal digital assistant 2 and also the mutual recognition between the control units of a personal digital assistant 2 and an automatic vending machine 1 are needed in order to prevent forgery of IC card 3, forgery of a personal digital assistant, the alteration of the data based on imitation of commo data, and exploitation of goods.
[0007] Conventionally, generally the approach using the random number as the approach of this mutual recognition is enforced. Between mutual equipment, it gives the control section of an automatic vending machine, and the both sides of a personal digital assistant the random-number generation means and common encryption/decryption key, enciphers delivery and its data with a common encryption key mutually against the random-number data generated to each other, respectively, and returns them to a partner here. As compared with the random-number data which decrypted the code data with the common key, and sent it first, if the same, it will judge that encryption/decryption key common to each other is shared, and being a just partner will be admited.
[0008]
[Problem(s) to be Solved by the Invention] As for the approach of mutual recognition using this random number, it becomes required conditions absolutely that the dependability of a random-number generation means, i.e., the generated random number, is not predicted by the holder in bad faith. However, since the time stump method which the conventional random-number generation means measures the time of day of the clock LSI built in each equipment, and makes the data random-number initial value, an M sequence method, a nonlinear combiner method, etc. are used, the time-of-day data of the neighborhood tend to be used by time-of-day presumption, and a time stump method has periodicity by the M sequence method, linearity is low and a problem is in safety.
[0009]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, then, invention of claim 1 The random-number data which are between two devices which have common encryption/decryption key, and one device generated to the device of another side Delivery, The device of another side which received it enciphers random-number data, and returns them to one device. In the mutual recognition equipment between the information machines and equipment which accept that a phase hand-loom machine is just when a device decrypts code data and while it was received is in agreement as compared with the original random-number data It is characterized by having a random-number generation means to measure the depression time amount of the alter operation key which one device has, and to generate a random number by making the value of the measuring time into initial value.
[0010] Invention of claim 2 holds the numeric value of a proper beforehand to the device of another side in invention of claim 1. After random-number data are sent to the device of another side from one device and it is enciphered and returned A device enciphers the numeric value of a proper and while delivery and it were received to one device returns the numeric value of the proper holding the device of another side to the device of another side. The device of another side which received it is characterized by accepting that a phase hand-loom machine is just, when code data are decrypted and it is in agreement as compared with the numeric value of the original proper.
[0011] In invention of claim 1 or claim 2, invention of claim 3 uses the device of another side as the IC card with which said personal digital assistant can be equipped while using one device as a personal digital assistant, and it is characterized by having a bottom time amount measurement means of a key press to measure the bottom time amount of a key press when the alter operation of the ID number to a personal digital assistant is made after IC card wearing, and to input into a random-number generation means.
[0012] In invention of claim 1 or claim 2, invention of claim 4 uses the device of another side as the automatic vending machine in which data transmission and reception are possible by non-contact [said / personal digital assistant and non-contact] while using one device as a personal digital assistant, and it is characterized by to have a bottom time-amount measurement means of a key press measures the bottom time amount of a key press when the alter operation of the ID number to a personal digital assistant is made in the state of both connection, and input into a random-number generation means.
[0013]

[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained along drawing. Drawing 1 is drawing showing the configuration at the time of applying this invention to the system by which a route man collects the sales of an automatic vending machine using the personal digital assistant which has infrared communication facility. This system consists of an automatic vending machine 1 and IC card 3 held by the individual (route man) who uses the personal digital assistant 2 in which the data exchange is possible, and a personal digital assistant 2 by non-contact by having the automatic vending machine 1 which can be used and infrared communication facility of cybermoney. In this system, after a route man inserts in a personal digital assistant 2 IC card 3 which is its own ID, subsequently inputs an ID number and it is recognized that IC card 3 is just to a personal digital assistant 2, the data of the sales and others by the cybermoney of an automatic vending machine 1 are collected to a personal digital assistant 2 by infrared ray communication, and those data are further moved and changed to a route man's IC card 3.

[0014] Here, it can save as hysteresis which it had when some troubles occurred because everybody have ID. Moreover, it can prevent that data are monitored by the holder in bad faith by having used infrared ray communication for the data communication between an automatic vending machine 1 and a personal digital assistant 2. That is, since directivity spreads, it is easy to monitor by the easy sensor in the case of an electromagnetic wave with long wavelength, such as wireless and a cable, but it is because infrared radiation has the merit which cannot be monitored since [that wavelength is comparatively short] directivity is narrow.

[0015] Drawing 2 is the block diagram showing the internal configuration of the personal digital assistant 2 of drawing 1 . So that it may be illustrated a personal digital assistant 2 Overall control CPU21 to perform and its program Even if it memorizes ROM23 and important data to memorize and a power source is shut off The communications control circuit 214 for performing E2ROM24, the transient-data storage memory RAM 25 for program working and IC card 3 which can be saved, and communications control, the clock control circuit 22 which carries out an international standard frequency output control, a reset circuit 215, It is constituted by the indicator 210 which are the power control circuit 216 for carrying out current supply to a card, the interface terminal 221, the card sensor section 222, and the user interface section, the display driver 29 for it, and the display-control circuit 28. It has the mutual recognition means 213 for judging that he is an owner with just keyboard 212 for a route man to input the command of the sales data collection of an automatic vending machine, its interface 211, and IC card 3.

[0016] The mutual recognition means 213 consists of a random-number generation means 231 and an encryption/decryption means 232, when IC card 3 is inserted by the command from the random-number generation means 231, it points to it so that a password may be entered from the display screen of an indicator 210, and it measures to order the time amount on which the keyboard 212 was pushed for 1 microsecond by the timer control means 26, and makes the value an initial random-number value with a binary representation. Moreover, if mutual recognition is materialized as a result of encryption/decryption means' 232 decrypting the received code, authorization of the communications control circuit 217 for communication with an automatic-vending-machine 1 side of operation will be attained. The communication with an automatic vending machine 1 is equipped with the infrared transceiver driver circuit 218 which are the infrared photogenic organ LED 219, an electric eye PD 220, and its driver circuit in order to use infrared radiation.

[0017] Drawing 3 is the block diagram showing the internal configuration of IC card 3 of drawing 1 . So that it may be illustrated IC card 3 Overall control CPU31 to perform and its program Even if it memorizes ROM34 and important data to memorize and a power source is shut off It has the mutual recognition means 39 for judging that he is an owner with just communications control circuit 37 for performing E2ROM33, the transient-data storage memory RAM 32 for program working and the personal digital assistant 2 which can be saved, and communications control, interface terminal 38, and personal digital assistant 2. The mutual recognition means 39 is constituted by the random-number generation means 36 and encryption/decryption means 35.

[0018] Drawing 4 is the block diagram showing the internal configuration of the automatic vending machine 1 of drawing 1 . The control section 10 to which an automatic vending machine 1 performs transmitting and receiving processing, such as sales data, to the main control section 112 of a high order is connected through the command control means 111 so that it may be illustrated. A control section 10 is equipped with the mutual recognition means 16 for judging that he is an owner with just communications control circuit 15 for performing E2ROM13, the transient-data storage memory RAM 14 for program working and the personal digital assistant 2 which can be saved, and communications control and personal digital assistant 2, even if it

memorizes CPU11 which performs overall control, ROM12 which memorizes the program, and important data and a power source is shut off. The mutual recognition means 16 consists of a random-number generation means 17 and an encryption/decryption means 18. Moreover, the communication with a personal digital assistant 2 is equipped with the infrared transceiver driver circuit 116 which are the infrared photogenic organ LED 19, an electric eye PD 110, and its driver circuit in order to use infrared radiation. In addition, the coin MEKKU means 113 and the BIRUBARI means 114 are elsewhere connected to the main control section 112.
[0019] Next, the processing in the case of inserting IC card 3 in a personal digital assistant 2, and attesting each other is explained. Drawing 5 is a flow chart which shows the mutual recognition processing between IC card 3 and a personal digital assistant 2. Hereafter, authentication processing is explained, referring to drawing 5 . First, if IC card 3 is set to a personal digital assistant 2, connection of IC card 3 will be recognized by the card sensor section 222 of a personal digital assistant 2. Then, in order to make IC card 3 into a working state, the power control circuit 216, the clock control circuit 22, and a reset circuit 215 are activated.
[0020] next, a card holder -- in this case -- a route man -- the screen display of the indicator 210 of a personal digital assistant 2 -- following -- principals, such as an authentication number, -- ID is inputted from a keyboard 212. At this time, by the timer control means 26, the time amount on which the keyboard 212 is pushed is measured, and it inputs into the random-number generation means 231 by making that value into an initial random-number value. The random-number generation means 231 generates the random-number value Rt based on the inputted initial random-number value, and sends it to IC card 3. In an IC card 3 side, using the same cryptographic key K, the encryption means 35 enciphers the random-number value Rt, and generates Code Fk (Rt). Code Fk (Rt) is returned to a personal digital assistant 2 from IC card 3.
[0021] A personal digital assistant 2 decrypts the returned code Fk (Rt) with the decryption means 232 using the same cryptographic key K, compares the value Rt' with the random-number value Rt currently held at the personal digital assistant 2, in the case of an inequality, recognizes it as what has inaccurate IC card 3, and discharges IC card 3. If in agreement, a trigger signal will be sent to IC card 3. The random-number generation means 36 will generate the random-number value Rc based on the initial random-number value of the proper currently held beforehand, and IC card 3 will send it to a personal digital assistant 2, if a trigger signal is sent. In a personal digital assistant 2 side, using the same cryptographic key K, the encryption means 232 enciphers the random-number value Rc, and generates Code Fk (Rc). Code Fk (Rc) is returned to IC card 3 from a personal digital assistant 2.
[0022] IC card 3 decrypts the returned code Fk (Rc) with the decryption means 35 using the same cryptographic key K, compares the value Rc' with the random-number value Rc currently held at the personal digital assistant 2, in the case of an inequality, recognizes it as what has the inaccurate personal digital assistant 2, and suspends processing of IC card 3. If in agreement, the same cryptographic key will be owned, mutual authentication will be materialized, and IC card 3 and a personal digital assistant 2 will send the command which starts processing of data transmission and reception from IC card 3 to a personal digital assistant 2.
[0023] Next, after the mutual recognition of IC card 3 and a personal digital assistant 2 is materialized, the processing in the case of attesting each other between a personal digital assistant 2 and an automatic vending machine 1 is explained. Drawing 6 is a flow chart which shows the mutual recognition processing between a personal digital assistant 2 and an automatic vending machine 1. Although, as for the mutual recognition between this personal digital assistant 2 and automatic vending machine 1, data are transmitted and received using infrared radiation, since the processing itself is the same as that of the flow chart of drawing 5 except that the numbers of the block by the side of an automatic vending machine 1 differ, detailed explanation is omitted. Also in this case, when authentication is abortive, both sides suspend future processings, but if authentication is materialized, the command which starts processing of data transmission and reception will be progressed to a personal digital assistant 2 from an automatic-vending-machine 1 side delivery and henceforth at processing of the data transmission and reception between a personal digital assistant 2 and an automatic vending machine 1.
[0024] As mentioned above, in this invention, the periodicity of the time amount which is pushing the keyboard for every route man is lost to difference random-number initial value each time by having measured the depression time amount of a keyboard and having considered as random-number initial value. Consequently, the safety of the random-number data used for the mutual recognition between a personal digital assistant 2 and the automatic vending machine 1 of a high order improves, and reproduction of fraudulent data is made into ****. Moreover, by using infrared ray communication between a personal digital assistant 2 and an automatic vending machine 1, data wire tapping by the holder in bad faith becomes difficult, and safety increases further.

[0025]
[Effect of the Invention] As stated above, in case according to this invention it is between two devices which have common encryption/decryption key, the random number of each other is enciphered and decrypted and a partner is attested, the bottom time amount of a key press of one device is measured, a random value becomes acquires and is hard to be expected by having used the measured value as initial value for generating a random number, and dependability improves.

[Translation done.]

TECHNICAL FIELD

[Field of the Invention] This invention relates to the mutual recognition equipment between the suitable information machines and equipment for the system which collects the sales information on an automatic vending machine, and money information especially using the personal digital assistant with which a route man has infrared communication facility about the mutual recognition equipment between the information machines and equipment used for cybermoney, an electronic clearing system, etc.

[Translation done.]

PRIOR ART

[Description of the Prior Art] Although the magnetic card has been conventionally used as a pachinko card, a telephone card, etc. as a prepaid card, since security is inadequate, the IC card which has high security is being used so that a magnetic card may also become a social problem by alteration etc. Moreover, the cybermoney using the CPU built-in IC card called a smart card and the system called electronic banking are advocated, and various kinds of experiments are conducted in recent years. There is a system by which a route man collects the sales of the automatic vending machine which can use cybermoney as the example using the personal digital assistant which has infrared communication facility. Specifically, cybermoney here is a pocketbook value memorized to the address of the arbitration of the storage of an automatic vending machine.
[0003] Drawing 1 shows the system concept, is equipped with the automatic vending machine 1 which can be used and infrared communication facility of cybermoney, and consists of an automatic vending machine 1 and IC card 3 held by the individual for whom the personal digital assistant 2 in which the data exchange is possible, and a personal digital assistant 2 are used by non-contact. In this system, the data of the sales and others by the cybermoney of an automatic vending machine 1 are collected by the personal digital assistant 2 by infrared ray communication, and collection of money is made by moving and changing those data to a route man's IC card 3 further. Drawing 7 is the block diagram showing the structure of a personal digital assistant 2 where conventional IC card 3 is inserted.
[0004] A personal digital assistant 2 Overall control CPU21 to perform and its program Even if it memorizes ROM23 and important data to memorize and a power source is shut off The communications control circuit 214 for performing E2ROM24, the transient-data storage memory RAM 25 for program working and IC card 3 which can be saved, and communications control, the clock control circuit 22 which carries out an international standard frequency output control, a reset circuit 215, It is constituted by the power control circuit 216 for carrying out current supply to a card, the interface terminal 221, the indicator 210 that is the user interface section, the display driver 29 for it, and the display-control circuit 28. It has the mutual recognition means 213 for judging that he is an owner with just keyboard 212 for a route man to input the command for automatic-vending-machine data collection, its interface 211, and IC card 3.
[0005] This mutual recognition means 213 will make values, such as that time of day, an initial random-number value with a binary representation, if it points so that a password may be entered from the display screen of an indicator 210 and a keyboard 212 is pushed, when it consists of a random-number generation means 231 and an encryption/decryption means 232 and IC card 3 is inserted by the command from the random-number generation means 231. Moreover, by the result to which encryption/decryption means 232 decrypted the received code, if mutual recognition is materialized, actuation of the communications control circuit 217 will be permitted and the communication by the side of an automatic vending machine 1 will be attained. The communication with an automatic vending machine 1 is equipped with the infrared transceiver driver circuit 218 which are the infrared photogenic organ LED 219, an electric eye PD 220, and its driver circuit in order to use infrared radiation.
[0006] Whether the system excellent in security by which a route man can collect with justice, without being stolen by the offender, the cybermoney, i.e., the electronic data, transposed to the conventional coin and a bill, is establishable poses a problem here. Therefore, the mutual recognition between IC card 3 and a personal digital assistant 2 and also the mutual recognition between the control units of a personal digital assistant 2 and an automatic vending machine 1 are needed in order to prevent forgery of IC card 3, forgery of a personal digital assistant, the alteration of the data based on imitation of commo data, and exploitation of goods.
[0007] Conventionally, generally the approach using the random number as the approach of this mutual

recognition is enforced. Between mutual equipment, it gives the control section of an automatic vending machine, and the both sides of a personal digital assistant the random-number generation means and common encryption/decryption key, enciphers delivery and its data with a common encryption key mutually against the random-number data generated to each other, respectively, and returns them to a partner here. As compared with the random-number data which decrypted the code data with the common key, and sent it first, if the same, it will judge that encryption/decryption key common to each other is shared, and being a just partner will be admited.

[Translation done.]

EFFECT OF THE INVENTION

[Effect of the Invention] As stated above, in case according to this invention it is between two devices which have common encryption/decryption key, the random number of each other is enciphered and decrypted and a partner is attested, the bottom time amount of a key press of one device is measured, a random value becomes acquires and is hard to be expected by having used the measured value as initial value for generating a random number, and dependability improves.

[Translation done.]

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] As for the approach of mutual recognition using this random number, it becomes required conditions absolutely that the dependability of a random-number generation means, i.e., the generated random number, is not predicted by the holder in bad faith. However, since the time stump method which the conventional random-number generation means measures the time of day of the clock LSI built in each equipment, and makes the data random-number initial value, an M sequence method, a nonlinear combiner method, etc. are used, the time-of-day data of the neighborhood tend to be used by time-of-day presumption, and a time stump method has periodicity by the M sequence method, linearity is low and a problem is in safety.

[Translation done.]

MEANS

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, then, invention of claim 1 The random-number data which are between two devices which have common encryption/decryption key, and one device generated to the device of another side Delivery, The device of another side which received it enciphers random-number data, and returns them to one device. In the mutual recognition equipment between the information machines and equipment which accept that a phase hand-loom machine is just when a device decrypts code data and while it was received is in agreement as compared with the original random-number data It is characterized by having a random-number generation means to measure the depression time amount of the alter operation key which one device has, and to generate a random number by making the value of the measuring time into initial value.
[0010] Invention of claim 2 holds the numeric value of a proper beforehand to the device of another side in invention of claim 1. After random-number data are sent to the device of another side from one device and it is enciphered and returned A device enciphers the numeric value of a proper and while delivery and it were received to one device returns the numeric value of the proper holding the device of another side to the device of another side. The device of another side which received it is characterized by accepting that a phase hand-loom machine is just, when code data are decrypted and it is in agreement as compared with the numeric value of the original proper.
[0011] In invention of claim 1 or claim 2, invention of claim 3 uses the device of another side as the IC card with which said personal digital assistant can be equipped while using one device as a personal digital assistant, and it is characterized by having a bottom time amount measurement means of a key press to measure the bottom time amount of a key press when the alter operation of the ID number to a personal digital assistant is made after IC card wearing, and to input into a random-number generation means.
[0012] In invention of claim 1 or claim 2, invention of claim 4 uses the device of another side as the automatic vending machine in which data transmission and reception are possible by non-contact [said / personal digital assistant and non-contact] while using one device as a personal digital assistant, and it is characterized by to have a bottom time-amount measurement means of a key press measures the bottom time amount of a key press when the alter operation of the ID number to a personal digital assistant is made in the state of both connection, and input into a random-number generation means.
[0013]
[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained along drawing. Drawing 1 is drawing showing the configuration at the time of applying this invention to the system by which a route man collects the sales of an automatic vending machine using the personal digital assistant which has infrared communication facility. This system consists of an automatic vending machine 1 and IC card 3 held by the individual (route man) who uses the personal digital assistant 2 in which the data exchange is possible, and a personal digital assistant 2 by non-contact by having the automatic vending machine 1 which can be used and infrared communication facility of cybermoney. In this system, after a route man inserts in a personal digital assistant 2 IC card 3 which is its own ID, subsequently inputs an ID number and it is recognized that IC card 3 is just to a personal digital assistant 2, the data of the sales and others by the cybermoney of an automatic vending machine 1 are collected to a personal digital assistant 2 by infrared ray communication, and those data are further moved and changed to a route man's IC card 3.
[0014] Here, it can save as hysteresis which it had when some troubles occurred because everybody have ID. Moreover, it can prevent that data are monitored by the holder in bad faith by having used infrared ray communication for the data communication between an automatic vending machine 1 and a personal digital

assistant 2. That is, since directivity spreads, it is easy to monitor by the easy sensor in the case of an electromagnetic wave with long wavelength, such as wireless and a cable, but it is because infrared radiation has the merit which cannot be monitored since [that wavelength is comparatively short] directivity is narrow.
[0015] Drawing 2 is the block diagram showing the internal configuration of the personal digital assistant 2 of drawing 1 . So that it may be illustrated a personal digital assistant 2 Overall control CPU21 to perform and its program Even if it memorizes ROM23 and important data to memorize and a power source is shut off The communications control circuit 214 for performing E2ROM24, the transient-data storage memory RAM 25 for program working and IC card 3 which can be saved, and communications control, the clock control circuit 22 which carries out an international standard frequency output control, a reset circuit 215, It is constituted by the indicator 210 which are the power control circuit 216 for carrying out current supply to a card, the interface terminal 221, the card sensor section 222, and the user interface section, the display driver 29 for it, and the display-control circuit 28. It has the mutual recognition means 213 for judging that he is an owner with just keyboard 212 for a route man to input the command of the sales data collection of an automatic vending machine, its interface 211, and IC card 3.
[0016] The mutual recognition means 213 consists of a random-number generation means 231 and an encryption/decryption means 232, when IC card 3 is inserted by the command from the random-number generation means 231, it points to it so that a password may be entered from the display screen of an indicator 210, and it measures to order the time amount on which the keyboard 212 was pushed for 1 microsecond by the timer control means 26, and makes the value an initial random-number value with a binary representation. Moreover, if mutual recognition is materialized as a result of encryption/decryption means' 232 decrypting the received code, authorization of the communications control circuit 217 for communication with an automatic-vending-machine 1 side of operation will be attained. The communication with an automatic vending machine 1 is equipped with the infrared transceiver driver circuit 218 which are the infrared photogenic organ LED 219, an electric eye PD 220, and its driver circuit in order to use infrared radiation.
[0017] Drawing 3 is the block diagram showing the internal configuration of IC card 3 of drawing 1 . So that it may be illustrated IC card 3 Overall control CPU31 to perform and its program Even if it memorizes ROM34 and important data to memorize and a power source is shut off It has the mutual recognition means 39 for judging that he is an owner with just communications control circuit 37 for performing E2ROM33, the transient-data storage memory RAM 32 for program working and the personal digital assistant 2 which can be saved, and communications control, interface terminal 38, and personal digital assistant 2. The mutual recognition means 39 is constituted by the random-number generation means 36 and encryption/decryption means 35.
[0018] Drawing 4 is the block diagram showing the internal configuration of the automatic vending machine 1 of drawing 1 . The control section 10 to which an automatic vending machine 1 performs transmitting and receiving processing, such as sales data, to the main control section 112 of a high order is connected through the command control means 111 so that it may be illustrated. A control section 10 is equipped with the mutual recognition means 16 for judging that he is an owner with just communications control circuit 15 for performing E2ROM13, the transient-data storage memory RAM 14 for program working and the personal digital assistant 2 which can be saved, and communications control and personal digital assistant 2, even if it memorizes CPU11 which performs overall control, ROM12 which memorizes the program, and important data and a power source is shut off. The mutual recognition means 16 consists of a random-number generation means 17 and an encryption/decryption means 18. Moreover, the communication with a personal digital assistant 2 is equipped with the infrared transceiver driver circuit 116 which are the infrared photogenic organ LED 19, an electric eye PD 110, and its driver circuit in order to use infrared radiation. In addition, the coin MEKKU means 113 and the BIRUBARI means 114 are elsewhere connected to the main control section 112.
[0019] Next, the processing in the case of inserting IC card 3 in a personal digital assistant 2, and attesting each other is explained. Drawing 5 is a flow chart which shows the mutual recognition processing between IC card 3 and a personal digital assistant 2. Hereafter, authentication processing is explained, referring to drawing 5 . First, if IC card 3 is set to a personal digital assistant 2, connection of IC card 3 will be recognized by the card sensor section 222 of a personal digital assistant 2. Then, in order to make IC card 3 into a working state, the power control circuit 216, the clock control circuit 22, and a reset circuit 215 are activated.
[0020] next, a card holder -- in this case -- a route man -- the screen display of the indicator 210 of a personal digital assistant 2 -- following -- principals, such as an authentication number, -- ID is inputted from a keyboard

212. At this time, by the timer control means 26, the time amount on which the keyboard 212 is pushed is measured, and it inputs into the random-number generation means 231 by making that value into an initial random-number value. The random-number generation means 231 generates the random-number value Rt based on the inputted initial random-number value, and sends it to IC card 3. In an IC card 3 side, using the same cryptographic key K, the encryption means 35 enciphers the random-number value Rt, and generates Code Fk (Rt). Code Fk (Rt) is returned to a personal digital assistant 2 from IC card 3.

[0021] A personal digital assistant 2 decrypts the returned code Fk (Rt) with the decryption means 232 using the same cryptographic key K, compares the value Rt' with the random-number value Rt currently held at the personal digital assistant 2, in the case of an inequality, recognizes it as what has inaccurate IC card 3, and discharges IC card 3. If in agreement, a trigger signal will be sent to IC card 3. The random-number generation means 36 will generate the random-number value Rc based on the initial random-number value of the proper currently held beforehand, and IC card 3 will send it to a personal digital assistant 2, if a trigger signal is sent. In a personal digital assistant 2 side, using the same cryptographic key K, the encryption means 232 enciphers the random-number value Rc, and generates Code Fk (Rc). Code Fk (Rc) is returned to IC card 3 from a personal digital assistant 2.

[0022] IC card 3 decrypts the returned code Fk (Rc) with the decryption means 35 using the same cryptographic key K, compares the value Rc' with the random-number value Rc currently held at the personal digital assistant 2, in the case of an inequality, recognizes it as what has the inaccurate personal digital assistant 2, and suspends processing of IC card 3. If in agreement, the same cryptographic key will be owned, mutual authentication will be materialized, and IC card 3 and a personal digital assistant 2 will send the command which starts processing of data transmission and reception from IC card 3 to a personal digital assistant 2.

[0023] Next, after the mutual recognition of IC card 3 and a personal digital assistant 2 is materialized, the processing in the case of attesting each other between a personal digital assistant 2 and an automatic vending machine 1 is explained. Drawing 6 is a flow chart which shows the mutual recognition processing between a personal digital assistant 2 and an automatic vending machine 1. Although, as for the mutual recognition between this personal digital assistant 2 and automatic vending machine 1, data are transmitted and received using infrared radiation, since the processing itself is the same as that of the flow chart of drawing 5 except that the numbers of the block by the side of an automatic vending machine 1 differ, detailed explanation is omitted. Also in this case, when authentication is abortive, both sides suspend future processings, but if authentication is materialized, the command which starts processing of data transmission and reception will be progressed to a personal digital assistant 2 from an automatic-vending-machine 1 side delivery and henceforth at processing of the data transmission and reception between a personal digital assistant 2 and an automatic vending machine 1.

[0024] As mentioned above, in this invention, the periodicity of the time amount which is pushing the keyboard for every route man is lost to difference random-number initial value each time by having measured the depression time amount of a keyboard and having considered as random-number initial value. Consequently, the safety of the random-number data used for the mutual recognition between a personal digital assistant 2 and the automatic vending machine 1 of a high order improves, and reproduction of fraudulent data is made into ****. Moreover, by using infrared ray communication between a personal digital assistant 2 and an automatic vending machine 1, data wire tapping by the holder in bad faith becomes difficult, and safety increases further.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is structure-of-a-system drawing which collects the sales of the automatic vending machine with which this invention is applied using a personal digital assistant.
[Drawing 2] It is the block diagram showing the internal configuration of the personal digital assistant of drawing 1 .
[Drawing 3] It is the block diagram showing the internal configuration of the IC card of drawing 1 .
[Drawing 4] It is the block diagram showing the internal configuration of the automatic vending machine of drawing 1 .
[Drawing 5] It is the flow chart which shows the mutual recognition processing between the IC card of drawing 1 , and a personal digital assistant.
[Drawing 6] It is the flow chart which shows the mutual recognition processing between the personal digital assistant of drawing 1 , and an automatic vending machine.
[Drawing 7] It is drawing showing the conventional example.
[Description of Notations]
1 Automatic Vending Machine
10 Control Section
11 CPU
12 ROM
13 E2ROM
14 RAM
15 Communications Control Circuit
16 Mutual Recognition Means
17 Random-Number Generation Means
18 Encryption/Decryption Means
19 Infrared Photogenic Organ LED
110 Electric Eye PD
111 Command Control Means
112 Main Control Section
113 Coin MEKKU Means
114 BIRUBARI Means
116 Infrared Transceiver Driver Circuit
2 Personal Digital Assistant
21 CPU
22 Clock Control Circuit
23 ROM
24 E2ROM
25 RAM
26 Timer Control Means
28 Display-Control Circuit
29 Display Driver
210 Drop
211 Interface

212 Keyboard
213 Mutual Recognition Means
214 Communications Control Circuit
215 Reset Circuit
216 Power Control Circuit
217 Communications Control Circuit
218 Infrared Transceiver Driver Circuit
219 Infrared Photogenic Organ LED
220 Electric Eye PD
221 Interface Terminal
222 Card Sensor Section
231 Random-Number Generation Means
232 Encryption/Decryption Means
3 IC Card
31 CPU
32 RAM
33 E2ROM
34 ROM
35 Encryption/Decryption Means
36 Random-Number Generation Means
37 Communications Control Circuit
38 Interface Terminal
39 Mutual Recognition Means

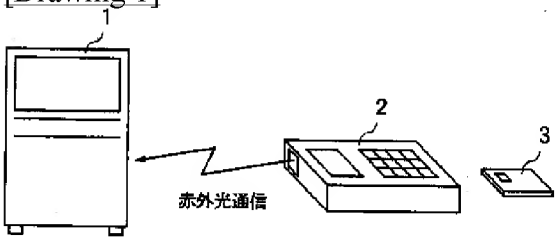
[Translation done.]

* NOTICES *

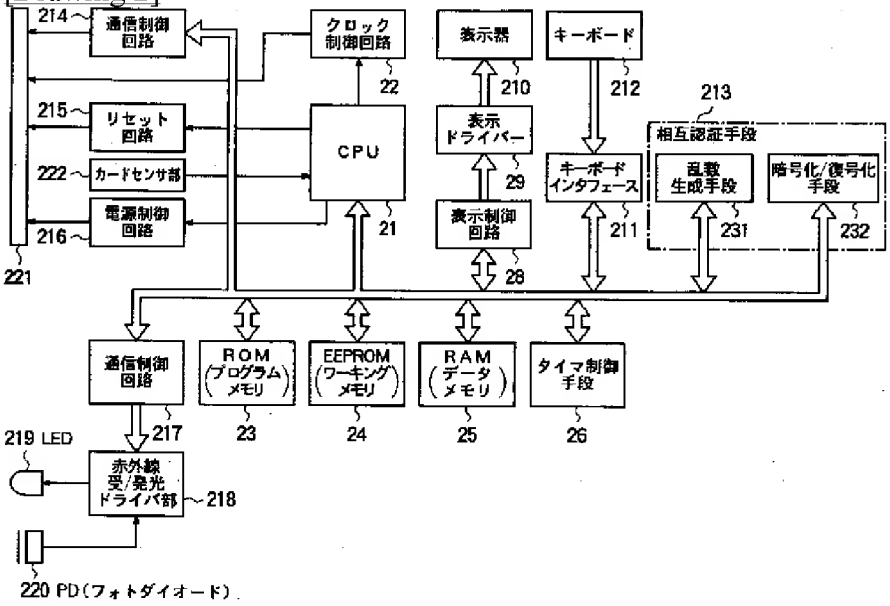
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

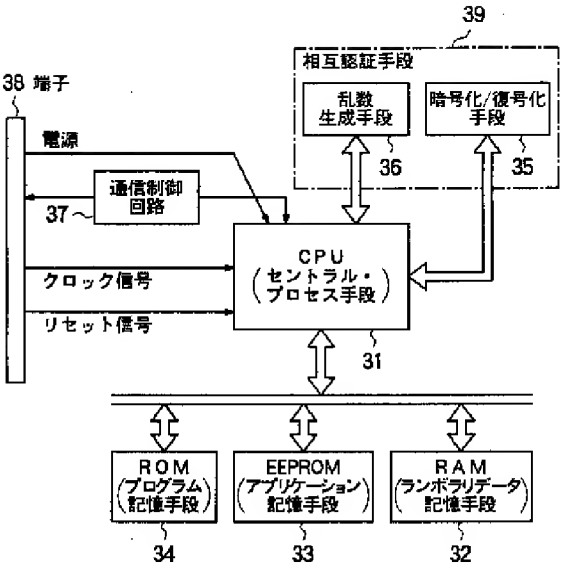
[Drawing 1]



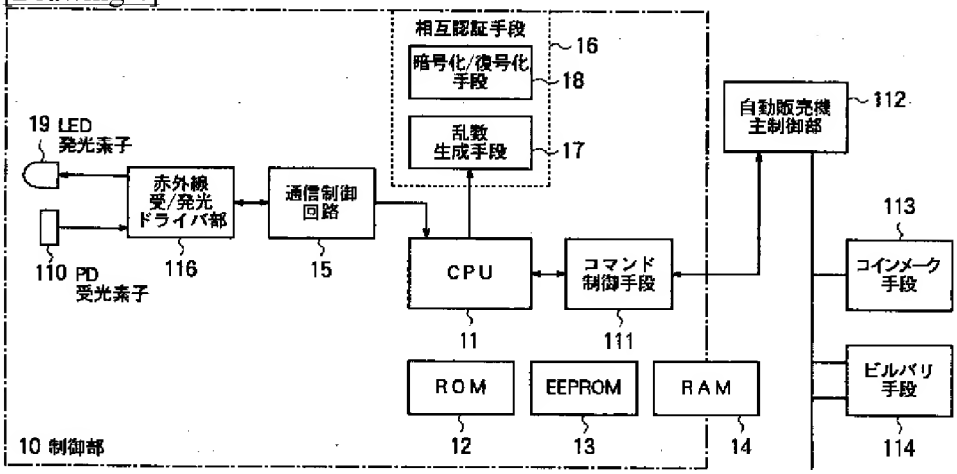
[Drawing 2]



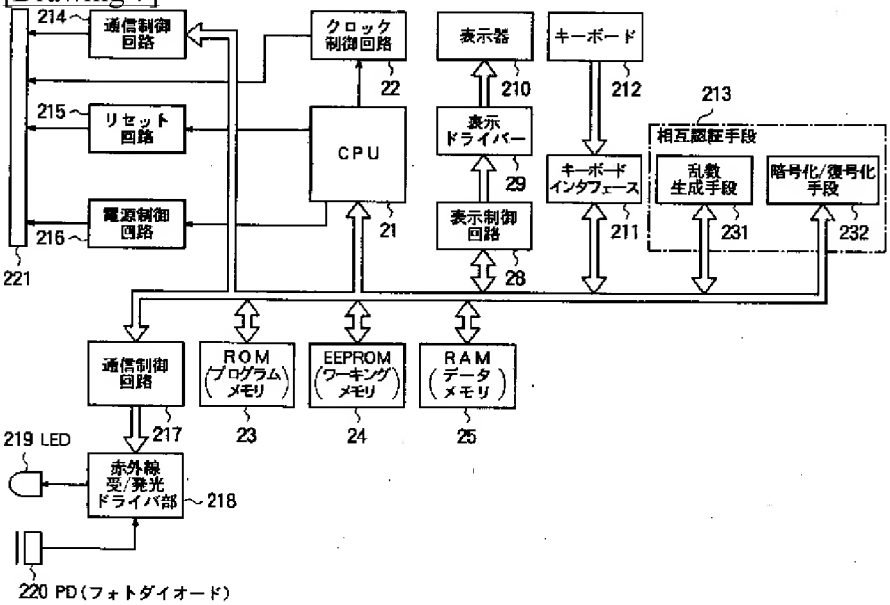
[Drawing 3]



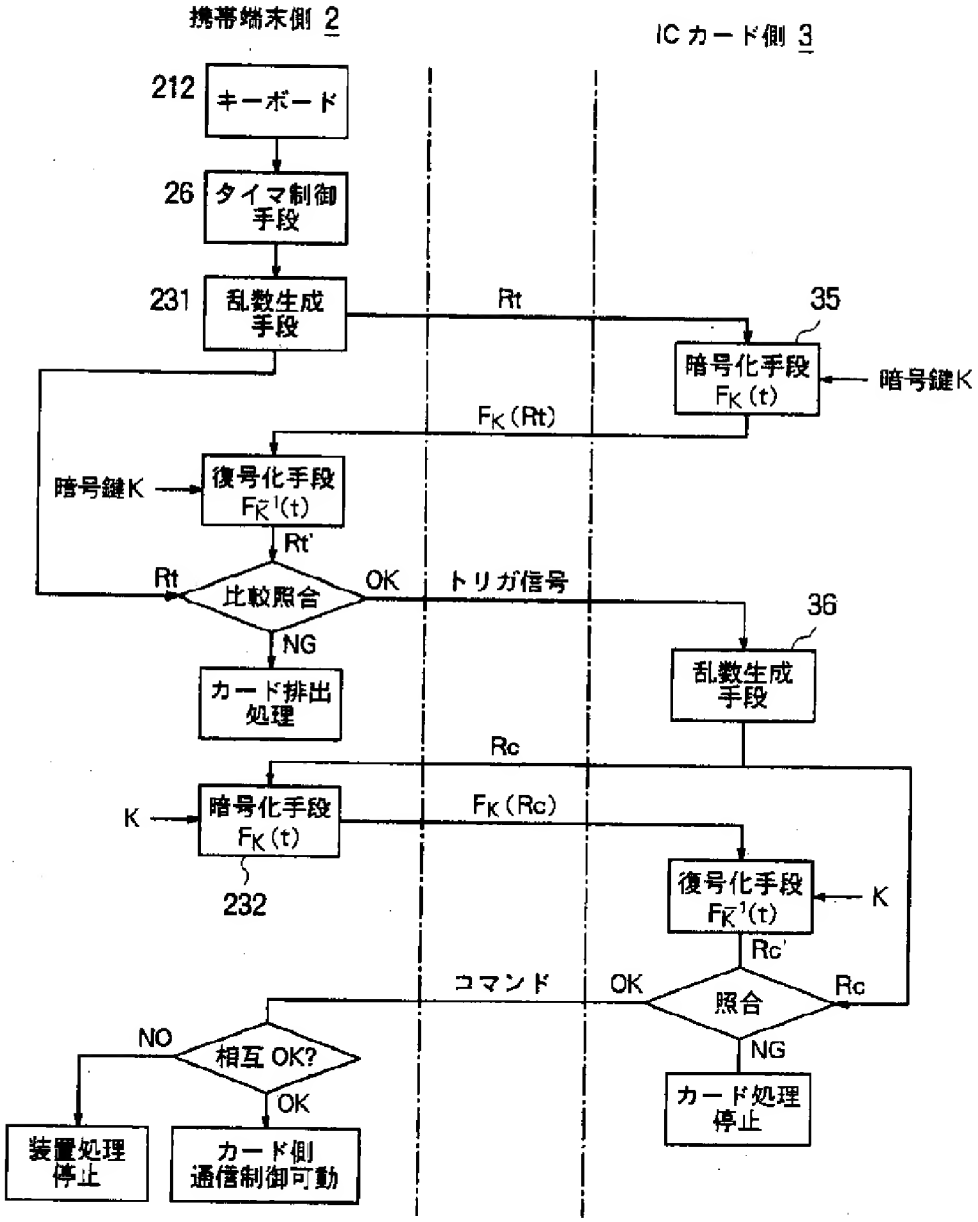
[Drawing 4]



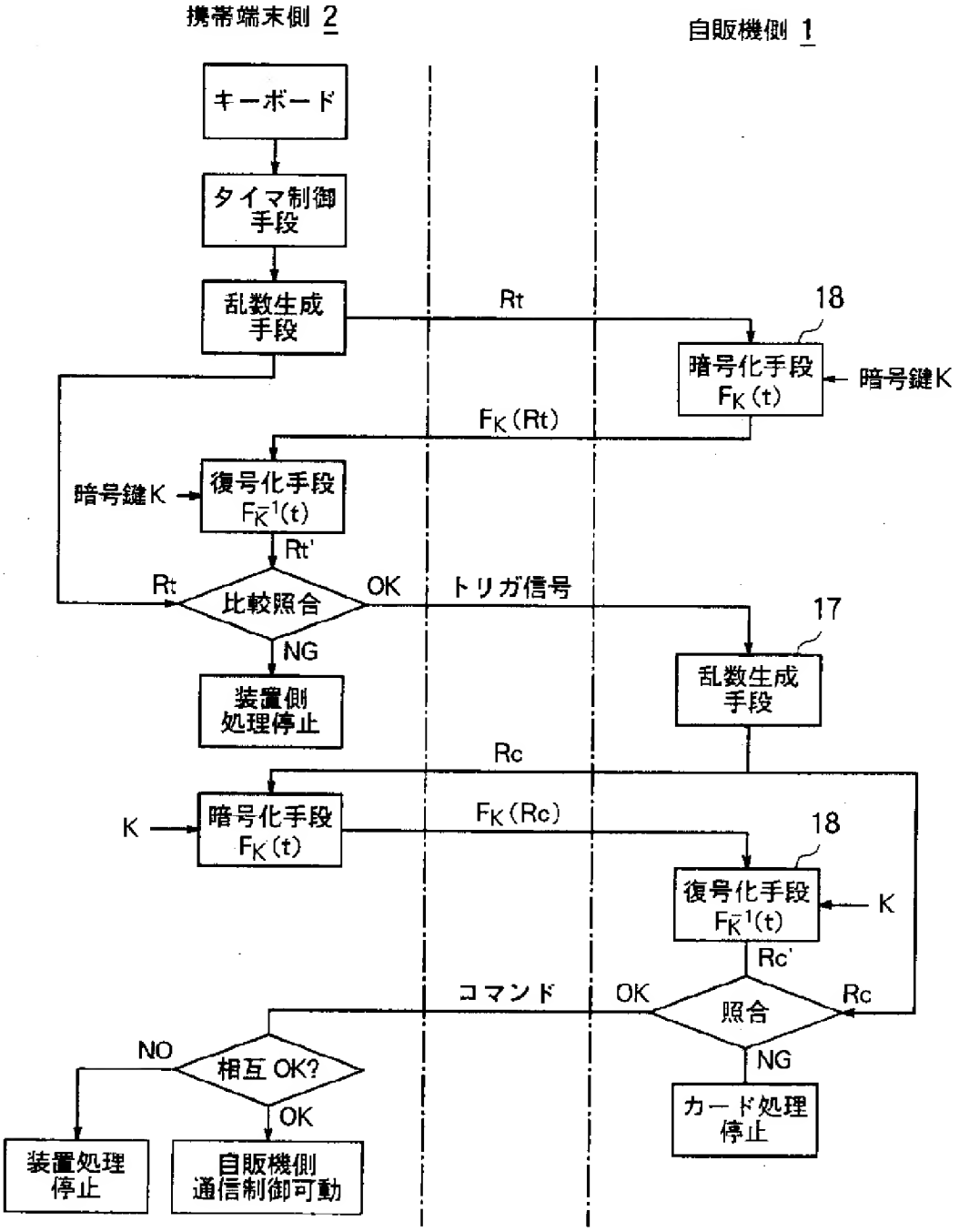
[Drawing 7]



[Drawing 5]


携帯端末側 2
ICカード側 3
212
キーボード
26
タイマ制御手段
231
乱数生成手段
Rt
35
暗号化手段 FK(t)
暗号鍵K
FK(Rt)
暗号鍵K
復号化手段 FK-1(t)
Rt'
Rt
比較照合
OK
トリガ信号
36
NG
カード排出処理
乱数生成手段
Rc
K
暗号化手段 FK(t)
FK(Rc)
232
復号化手段 FK-1(t)
K
Rc'
コマンド
OK
照合
Rc
NO
相互 OK?
NG
カード処理停止
OK
装置処理停止
カード側通信制御可動

[Drawing 6]



[Translation done.]